

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344445

(43)Date of publication of application : 29.11.2002

(51)Int.Cl.

H04L 9/32
G09C 1/00

(21)Application number : 2001-149331

(71)Applicant : NEC CORP

(22)Date of filing : 18.05.2001

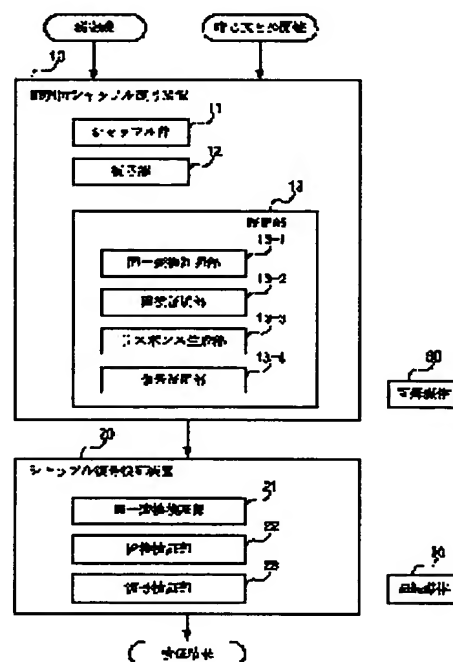
(72)Inventor : FURUKAWA JUN

(54) SHUFFLE-DECODING SYSTEM WITH CERTIFICATION AND METHOD THEREFOR, AND SHUFFLE DECODING VERIFICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a shuffle decoding system with certification capable of efficiently processing calculation quantity and certification statement quantity.

SOLUTION: This system is provided with a shuffle-decoding device, having certification for generating a shuffle decoding statement and a shuffle decoding certification statement and a shuffle-decoding verifying device for verifying the shuffle decoding processing, by referring to the generated shuffle decoding statement and the shuffle decoding certification statement. The shuffle-decoding device with certification accepts the input of a plurality of cryptographic statements and a public key and the secret key of the decoding; generates the shuffled cryptographic statements by enciphering the cryptographic statements with the public key by exchanging the order of the cryptographic statement; generates shuffle decoded statement statements by decoding the shuffled cryptographic statements with the secret key; generates a response to be referred to when executing certification, and generates a certification statement for certifying the validity of the exchange of the order of the cryptographic statements, the encipherment, and the decoding for generating the shuffle decoded statements based on the response; and output the respective generated certification statements and responses as shuffle-decoding certification statements.



LEGAL STATUS

[Date of request for examination]

12.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-344445
(P2002-344445A)

(43) 公開日 平成14年11月29日 (2002. 11. 29)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L 9/32		G 0 9 C 1/00	6 4 0 C 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 C

審査請求 未請求 請求項の数19 O L (全 17 頁)

(21) 出願番号 特願2001-149331 (P2001-149331)

(22) 出願日 平成13年5月18日 (2001. 5. 18)

(71) 出願人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者 古川 潤

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100093595

弁理士 松本 正夫

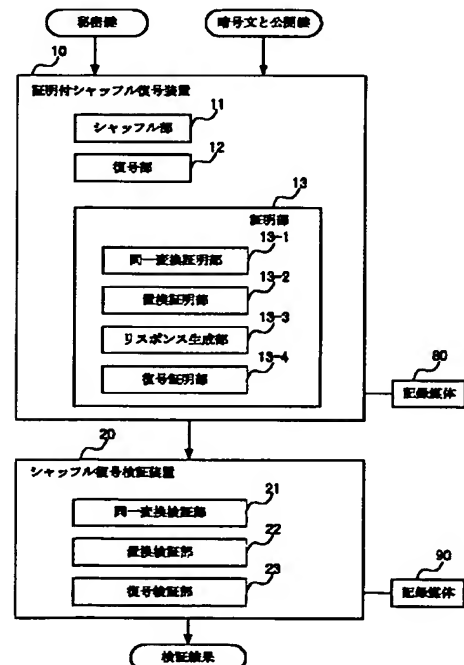
Fターム (参考) 5J104 AA18 JA29 KA08 NA02 NA09
NA10

(54) 【発明の名称】 証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法

(57) 【要約】 (修正有)

【課題】 計算量と証明文量を効率良く処理する証明付シャッフル復号システムの提供。

【解決手段】 シャッフル復号文を生成し、且つシャッフル復号証明文を生成する証明付シャッフル復号装置と、生成されたシャッフル復号文とシャッフル復号証明文とを参照し、シャッフル復号処理の検証を行うシャッフル復号検証装置を備え、証明付シャッフル復号装置は、複数の暗号文と、公開鍵と復号の秘密鍵との入力を受け付け、暗号文の順番を入れ替えて公開鍵により暗号化したシャッフル済み暗号文を、秘密鍵により復号してシャッフル復号文を生成し、証明において参照するリスポンスを生成し、リスポンスに基づいて、シャッフル復号文を生成する為の順番の入れ替えと暗号化と復号とにおけるそれぞれの正当性を証明する証明文を生成し、生成された各証明文とリスポンスとを、シャッフル復号証明文として出力する事の特徴とする。



【特許請求の範囲】

【請求項1】 複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号装置において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする証明付シャッフル復号装置。

【請求項2】 前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする請求項1に記載の証明付シャッフル復号装置。

【請求項3】 前記証明部は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項2に記載の証明付シャッフル復号装置。

【請求項4】 複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とするシャッフル復号検証装置。

【請求項5】 前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項4に記載のシャッフル復号検証装置。

【請求項6】 複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号方法において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シ

シャッフル復号証明文として出力することを特徴とする証明付シャッフル復号方法。

【請求項7】 前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフルステップと、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号ステップと、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明ステップを備えることを特徴とする請求項6に記載の証明付シャッフル復号方法。

【請求項8】 前記証明ステップは、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明ステップと、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明ステップと、前記同一変換証明ステップと置換証明ステップに対する前記リスポンスを生成するリスポンス生成ステップと、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明ステップを備え、前記同一変換証明ステップと、前記置換証明ステップと、前記リスポンス生成ステップと、前記復号証明ステップにおいて生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項7に記載の証明付シャッフル復号方法。

【請求項9】 複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証方法において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とするシャッフル復号検証方法。

【請求項10】 前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証ステップと、前記シャッフル復号証明文の入力と前記同一変換検証ステップで生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証ステップと、前記シャッフル復号証明文と前記同一変換検証ステップで生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証ステップとを備え、前記同一変換検証ステップと、前記置換検証ステップと、前記復号検証ステップのそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項9に記載のシャッフル復号検証方法。

【請求項11】 複数の暗号文をシャッフル復号して生成したシャッフル復号文の、前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成し、前記シャッフル復号証明文に基づいて前記シャッフル復号の処理が正しく行われたことを検証する証明付シャッフル復号システムにおいて、前記複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号証明文を生成する証明付シャッフル復号装置と、生成された前記シャッフル復号文と、当該シャッフル復号文の前記シャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置を備え、前記証明付シャッフル復号装置は、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする証明付シャッフル復号システム。

【請求項12】 前記証明付シャッフル復号装置は、前記複数の暗号文と前記公開鍵との入力を受けて、前記

複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、

前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする請求項11に記載の証明付シャッフル復号システム。

【請求項13】 前記証明付シャッフル復号装置の前記証明部は、

前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、

前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、

前記同一変換証明部と置換証明部に対する前記リスポンスを生成するリスポンス生成部と、

前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明部を備え、

前記同一変換証明部と、前記置換証明部と、前記リスポンス生成部と、前記復号証明部により生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする請求項12に記載の証明付シャッフル復号システム。

【請求項14】 前記シャッフル復号検証装置は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、

前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、

前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部

とを備え、

前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする請求項11から請求項13のいずれか一つに記載の証明付シャッフル復号システム。

【請求項15】 コンピュータを制御することにより、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号プログラムにおいて、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、

前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、

前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力する処理を実行させることを特徴とする証明付シャッフル復号プログラム。

【請求項16】 前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル処理と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号処理と、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明処理を実行させることを特徴とする請求項15に記載の証明付シャッフル復号プログラム。

【請求項17】 前記証明処理は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明処理と、

前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明処理と、

前記同一変換証明処理と置換証明処理に対する前記リスポンスを生成するリスポンス生成処理と、

前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号

10

20

30

40

50

証明処理と、
前記同一変換証明処理と、前記置換証明処理と、前記リス
ポンス生成処理と、前記復号証明処理において生成され
た各前記証明文と前記リスポンスの全てを、前記シャ
ッフル復号証明文として出力する処理を実行させること
を特徴とする請求項16に記載の証明付シャッフル復号
プログラム。

【請求項18】 コンピュータを制御することにより、
複数の暗号文をシャッフル復号して生成されたシャッ
フル復号文を、当該シャッフル復号文の前記シャッフル復
号の処理が正しく行われたことを証明する証明文である
シャッフル復号証明文を参照し、前記シャッフル復号の
処理が正しく行われたことを検証するシャッフル復号検
証プログラムにおいて、
前記シャッフル復号証明文は、
証明において参照するリスポンスと、
前記暗号文の順番を入れ替えて前記公開鍵により暗号化
したシャッフル済み暗号文を前記秘密鍵により復号する
処理である前記シャッフル復号文を生成する処理の、正
当性を証明するための前記リスポンスに基づいて生成され
た証明文とを含むことを特徴とするシャッフル復号検
証プログラム。

【請求項19】 前記シャッフル復号証明文と前記暗号
文と前記公開鍵と前記シャッフル復号文との入力を受け
て、前記順番の入れ替え及び前記暗号化における当該暗
号文の変換内容の情報を証明文の作成側が持っているこ
とを検証し、チャレンジを生成し、更に、前記入力され
る暗号文が複数の整数の要素である場合には、それぞれの
要素が同じ順番の入れ替えと暗号化の処理とを受けて
いることを検証する同一変換検証処理と、
前記シャッフル復号証明文の入力と前記同一変換検証処
理で生成されたチャレンジの入力とを受けて、前記暗号
文に対して順番の入れ替えが正しくなされたことを検証
する置換検証処理と、
前記シャッフル復号証明文と前記同一変換検証処理で生
成されたチャレンジとの入力を受けて、前記シャッフル
復号文が、前記シャッフル済み暗号文を前記秘密鍵を用
いて正しく復号して生成されたことを検証する復号検証
処理と、
前記同一変換検証処理と、前記置換検証処理と、前記復
号検証処理のそれぞれにおいて、全て正当と検証された
場合に限り、前記シャッフル復号文が入力された前記暗
号文を正しくシャッフル復号したと判定する処理を実行
させることを特徴とする請求項18に記載のシャッフル
復号検証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、匿名通信路の構成
等において使われる、証明付シャッフル及び証明付復号
を処理する証明付シャッフル復号システムと証明付シャ

ッフル復号方法、シャッフル復号検証方法に関する。

【0002】

【従来の技術】【従来の証明付シャッフル】従来の証明
付シャッフルの技術には、例えば、特願2000-05
9091号（以下、文献1）に記載された従来技術がある。

【0003】図6は、文献1に記載された従来技術の構
成を示す図である。なお、以下各図面中においては、合
流する矢印は、矢印の元の側における情報が全て集まっ
て矢印の先へ送られることを意味し、分岐する矢印は、
矢印の元の側の情報の全て又は一部がそれぞれの矢印の
先へ送られることを意味する。

【0004】また、本明細書におけるシャッフルは、文
献1においては再暗号シャッフルと呼んでいる。ここ
で、シャッフルとは、入力された暗号文をその順序を入
れ替えて再び暗号化することである。

【0005】図6においては、まず、暗号文と公開鍵1
00がシャッフルステップ101に入力されてシャッフル
される。この時入力された暗号文100とシャッフル
を特定する情報であるシャッフル情報102が同一変換
証明ステップ103に送られ、シャッフル情報102が
置換証明ステップ104に送られる。同一変換証明ステ
ップ103は、同一変換証明文105を生成し出力する
と同時に、証明文生成に使用した乱数106を置換証明
ステップ104に送る。置換証明ステップ104は置換
証明文107を出力する。リスポンス生成ステップ10
8には、同一変換証明文105と置換証明文104と暗
号文と公開鍵100とシャッフル済み暗号文109とを
入力し、同一変換証明文105と置換証明文104と暗
号文とにリスポンスを加えてシャッフル証明文110を
生成し出力する。

【0006】同一変換証明文105は、リスポンスと合
さって、入力文の順番の入れ替えや暗号化である暗号文
の変換内容の知識を持っていることの証明であると同時に、
入力される暗号文が複数の整数の要素となる場合は
それぞれの要素が同じ順番の入れ替えと対応する暗号化
の処理とを受けたことの証明でもある。置換証明文10
7は、リスポンスと合さって、入力される暗号文に対し
ての、順番の入れ替えが正しくなされたことの証明であ
る。

【0007】このシャッフルの処理が正当であることを
証明するために、文献1では同一変換証明ステップと置
換証明ステップの二つの証明ステップを用いている。こ
の証明対象の分割により文献1ではシャッフル証明文生
成の効率化を達成している。

【0008】【従来の証明付復号】従来の証明付復号の
技術には、例えば、特開平08-263575号公報
（以下、文献2）に開示された従来技術がある。

【0009】図7は、文献2に開示された従来技術の構
成を示す図である。図7を参照すると、まず、シャッフル

ル済み暗号文 200 と秘密鍵 201 とが、復号ステップ 203 に入力されて復号される。この時入力されたシャッフル済み暗号文 200 と秘密鍵 201 と、複合されて得られた復号文 204 とが、復号証明ステップ 205 に送られる。復号証明ステップ 205 は、これらの情報より復号証明文 206 を出力する。

【0010】ここで、復号とは、暗号文を分散所持されている秘密鍵の一部を使って、部分的に暗号文を復号することであり、秘密鍵の一部を全て用いて復号を繰り返すと完全な復号がなされる。

【0011】〔従来の技術による、証明付シャッフル復号方法〕文献 1 の証明付シャッフルの技術と、文献 2 の証明付復号の技術とを合わせることにより、証明付シャッフル復号方法を構成することができる。

【0012】図 8 は、文献 1 と文献 2 の従来技術を単純につなげることにより構成された証明付シャッフル復号方法を示す図である。この方法では、シャッフル済み暗号文 304 がシャッフル復号証明文 316 に含まれていることと、シャッフル済み暗号文 304 が復号証明ステップに入力されることと、レスポンス生成ステップから

【0013】

【発明が解決しようとする課題】上述したように従来の技術では、以下に述べるような問題点があった。

【0014】入力された暗号文をシャッフルし、かつそのシャッフルされた結果に復号を施して復号文を出力し、更にその処理の正当性証明文を生成して出力する方法を考える。これは、前述のように、文献 1 と文献 2 の従来技術を組み合わせることにより匿名通信路を構成することができるが、この手法では、不要な情報であるシャッフル済み暗号文が正当性の証明のために必要となり、これを出力する必要がある。暗号文の数が多い場合等、このように不要なシャッフル済み暗号文を出力することは、証明文量を増大させ通信の効率を悪くする。

【0015】また、文献 2 の従来技術では、証明文生成のために計算量の大きい冪乗剰余演算を暗号文数に比例して行わなければならない。そのためにシャッフル復号の効率を悪くしている。

【0016】本発明の第 1 の目的は、上記従来技術の欠点を解決し、文献 1 と文献 2 を組み合わせた方式であって、シャッフル済み暗号文を出力する必要がなく、かつ計算量と証明文量を共に少なく抑え効率の良い証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法を提供することである。

【0017】本発明の第 2 の目的は、上記従来技術の欠点を解決し、冪乗剰余演算の回数及び計算量を大きく削減し、更なる高速化を実現する証明付シャッフル復号システムと証明付シャッフル復号方法、シャッフル復号検証方法を提供することである。

【0018】

【課題を解決するための手段】上記目的を達成するため本発明の証明付シャッフル復号装置は、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号装置において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するレスポンスを生成し、前記レスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記レスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【0019】請求項 2 の本発明の証明付シャッフル復号装置は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする。

【0020】請求項 3 の本発明の証明付シャッフル復号装置は、前記証明部は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、前記同一変換証明部と置換証明部に対する前記レスポンスを生成するレスポンス生成部と、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記レスポンスに基づく証明文を生成する復号証明部を備え、前記同一変換証明部と、前記置換証明部と、前記レスポンス生成部と、前記復号証明部により生成された各前記証明文と前記レスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【0021】請求項 4 の本発明のシャッフル復号検証装置は、複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル

10

20

30

40

50

復号検証装置において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【0022】請求項5の本発明のシャッフル復号検証装置は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【0023】請求項6の本発明の証明付シャッフル復号方法は、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号方法において、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するリスポンスを生成し、前記リスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記リスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【0024】請求項7の本発明の証明付シャッフル復号方法は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフルステップと、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号ステップと、

前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明ステップを備えることを特徴とする。

【0025】請求項8の本発明の証明付シャッフル復号方法は、前記証明ステップは、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明ステップと、前記入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明ステップと、前記同一変換証明ステップと置換証明ステップに対する前記リスポンスを生成するリスポンス生成ステップと、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記リスポンスに基づく証明文を生成する復号証明ステップを備え、前記同一変換証明ステップと、前記置換証明ステップと、前記リスポンス生成ステップと、前記復号証明ステップにおいて生成された各前記証明文と前記リスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【0026】請求項9の本発明のシャッフル復号検証方法は、複数の暗号文をシャッフル復号して生成されたシャッフル復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証方法において、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【0027】請求項10の本発明のシャッフル復号検証方法は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証ステップと、前記シャッフル復号証明文の入力と前記同一変換検証ステップで生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証ステップと、前記シャッフル復号証明文と前記同一変換検証ステップで生成されたチャレンジとの入力を受け

て、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証ステップとを備え、前記同一変換検証ステップと、前記置換検証ステップと、前記復号検証ステップのそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【0028】請求項11の本発明の証明付シャッフル復号システムは、複数の暗号文をシャッフル復号して生成したシャッフル復号文の、前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成し、前記シャッフル復号証明文に基づいて前記シャッフル復号の処理が正しく行われたことを検証する証明付シャッフル復号システムにおいて、前記複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号証明文を生成する証明付シャッフル復号装置と、生成された前記シャッフル復号文と、当該シャッフル復号文の前記シャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証装置を備え、前記証明付シャッフル復号装置は、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するレスポンスを生成し、前記レスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記レスポンスとを、前記シャッフル復号証明文として出力することを特徴とする。

【0029】請求項12の本発明の証明付シャッフル復号システムは、前記証明付シャッフル復号装置は、前記複数の暗号文と前記公開鍵との入力を受けて、前記複数の暗号文の順番を入れ替えて前記公開鍵により暗号化することにより、前記複数のシャッフル済み暗号文を生成するシャッフル部と、前記複数のシャッフル済み暗号文と前記秘密鍵との入力を受けて、前記シャッフル済み暗号文を前記秘密鍵により復号した前記複数のシャッフル復号文を生成する復号部と、前記複数の暗号文と前記公開鍵と前記秘密鍵との入力を受けて、前記シャッフル復号証明文を生成する証明部を備えることを特徴とする。

【0030】請求項13の本発明の証明付シャッフル復号システムは、前記証明付シャッフル復号装置の前記証明部は、前記順番の入れ替えにおける前後の対応関係と前記暗号化に使った乱数とを知っていることを証明する証明文を生成し、かつ、前記入力される暗号文が複数の整数の要素から成る場合には、更にそれぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明する証明文を生成する同一変換証明部と、前記入力さ

れる暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する置換証明部と、前記同一変換証明部と置換証明部に対する前記レスポンスを生成するレスポンス生成部と、前記シャッフル済み暗号文が前記秘密鍵を用いて正しく復号されて前記シャッフル復号文が生成されたことを証明する、前記レスポンスに基づく証明文を生成する復号証明部を備え、前記同一変換証明部と、前記置換証明部と、前記レスポンス生成部と、前記復号証明部により生成された各前記証明文と前記レスポンスの全てを、前記シャッフル復号証明文として出力することを特徴とする。

【0031】請求項14の本発明の証明付シャッフル復号システムは、前記シャッフル復号検証装置は、前記シャッフル復号証明文と前記暗号文と前記公開鍵と前記シャッフル復号文との入力を受けて、前記順番の入れ替え及び前記暗号化における当該暗号文の変換内容の情報を証明文の作成側が持っていることを検証し、チャレンジを生成し、更に、前記入力される暗号文が複数の整数の要素である場合には、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けていることを検証する同一変換検証部と、前記シャッフル復号証明文の入力と前記同一変換検証部で生成されたチャレンジの入力とを受けて、前記暗号文に対して順番の入れ替えが正しくなされたことを検証する置換検証部と、前記シャッフル復号証明文と前記同一変換検証部で生成されたチャレンジとの入力を受けて、前記シャッフル復号文が、前記シャッフル済み暗号文を前記秘密鍵を用いて正しく復号して生成されたことを検証する復号検証部とを備え、前記同一変換検証部と、前記置換検証部と、前記復号検証部のそれぞれにおいて、全て正当と検証された場合に限り、前記シャッフル復号文が入力された前記暗号文を正しくシャッフル復号したと判定することを特徴とする。

【0032】請求項15の本発明の証明付シャッフル復号プログラムは、コンピュータを制御することにより、複数の暗号文をシャッフル復号してシャッフル復号文を生成し、かつ前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を生成する証明付シャッフル復号プログラムにおいて、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を、前記秘密鍵により復号して前記シャッフル復号文を生成し、前記証明において参照するレスポンスを生成し、前記レスポンスに基づいて、前記シャッフル復号文を生成するための前記順番の入れ替えと前記暗号化と前記復号とにおけるそれぞれの正当性を証明する証明文を生成し、前記生成された各証明文と前記レスポンスとを、前記シャッフル復号証明文として出力する処理を実行させることを特徴とする。

【0033】請求項18の本発明のシャッフル復号検証プログラムは、コンピュータを制御することにより、複数の暗号文をシャッフル復号して生成されたシャッフル

復号文を、当該シャッフル復号文の前記シャッフル復号の処理が正しく行われたことを証明する証明文であるシャッフル復号証明文を参照し、前記シャッフル復号の処理が正しく行われたことを検証するシャッフル復号検証プログラムにおいて、前記シャッフル復号証明文は、証明において参照するリスポンスと、前記暗号文の順番を入れ替えて前記公開鍵により暗号化したシャッフル済み暗号文を前記秘密鍵により復号する処理である前記シャッフル復号文を生成する処理の、正当性を証明するための前記リスポンスに基づいて生成された証明文とを含むことを特徴とする。

【0034】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0035】〔証明付シャッフル復号方法〕本発明の証明付シャッフル復号においては、まず、暗号文と公開鍵と秘密鍵とを入力して、その暗号文と公開鍵からシャッフル済み暗号文を生成し、そのシャッフル済み暗号文を秘密鍵により復号して復号文を生成する。

【0036】次に、証明付シャッフル方法（証明付暗号シャッフル方法）を用いて、シャッフル済み暗号文とシャッフル証明文を生成する。この証明付シャッフルの処理は、例えば、文献1に記載された従来の技術を持ちいることができる。但し、本発明においては、証明文生成時のチャレンジ（文献1では挑戦値と記述）を生成する時に、シャッフル済み暗号文の代わりに復号文を用いる。

【0037】次に、検証仮定にてシャッフル済み暗号文の代わりに復号文を用いた場合に生じることによる検証式の差分を生成し、これをシャッフル証明文に加える。

【0038】次に、前記差分が正当に作成されたことの証明文を、復号証明文として生成する。前記シャッフル証明文と復号証明文を合わせてシャッフル復号証明文とし、この復号文とシャッフル復号証明文とを出力する。

【0039】〔シャッフル復号検証方法〕本発明のシャッフル復号検証においては、まず、暗号文と公開鍵と復号文とシャッフル復号証明文とを入力する。ここで本発明では、文献1のシャッフル検証におけるシャッフル済み暗号文の代わりに、復号文を入力して検証を行う。但し、シャッフル復号証明文に含まれる「検証仮定において、シャッフル済み暗号文の代わりに復号文を用いたために生じる検証式の差分」を利用して、検証式を修正して用いる。次に、前記差分の正当性を検証する。二つの検証（復号文を用いたシャッフル検証と、検証式の差分の正当性の検証）の結果が共に「正当」であれば、シャッフル復号の検証結果として「正当」を、そうでなければ「不当」を出力する。

【0040】図1は、本発明の一実施の形態による証明付シャッフル復号システムの構成を示すブロック図である。図1を参照すると、本実施の形態の証明付シャッ

ル復号システムは、証明文を生成する側の装置である証明付シャッフル復号装置10と、証明文を基に検証を行う側の装置であるシャッフル復号検証装置20を備えている。

【0041】証明付シャッフル復号装置10は、シャッフル部11、復号部12、証明部13を備えている。

【0042】シャッフル部11は、複数の暗号文と公開鍵との入力を受けて、入力された複数の暗号文の順番を入れ替えて、その結果を公開鍵により暗号化した複数のシャッフル済み暗号文を生成する。

【0043】復号部12は、シャッフル部11により生成された複数のシャッフル済み暗号文と、秘密鍵の入力を受けて、シャッフル済み暗号文を秘密鍵により復号した複数の復号文を生成し出力する。

【0044】証明部13は、複数の暗号文と公開鍵と秘密鍵とに基づいて証明文を生成する。証明部13は、更に同一変換証明部13-1、置換証明部13-2、リスポンス生成部13-3、復号証明部13-4を備えている。

【0045】同一変換証明部13-1は、シャッフル部11による順番の入れ替えの前後の対応関係と、暗号化に使った乱数とを知っていることを証明する（ゼロ知識証明を行う）証明文を生成する。また、同一変換証明部13-1は、入力される暗号文が複数の整数の要素からなる場合には、それぞれの要素が同じ順番の入れ替えをされ同じ乱数で処理されたことを証明するための証明文も生成する。

【0046】置換証明部13-2は、入力される暗号文に対しての、順番の入れ替えが正しくなされたことを証明する証明文を生成する。リスポンス生成部13-3は、同一変換証明部13-1と置換証明部13-2に対するリスポンスを生成する。復号証明部13-4は、シャッフル済み暗号文が、秘密鍵を用いて正しく復号されて復号文が生成されたことを証明する証明文を生成する。

【0047】そして、証明付シャッフル復号装置10は、同一変換証明部13-1、置換証明部13-2、リスポンス生成部13-3、復号証明部13-4により生成された証明文とリスポンスの全てを、シャッフル復号の証明文として出力する。

【0048】シャッフル復号検証装置20は、同一変換検証部21、置換検証部22、復号検証部23を備えている。

【0049】同一変換検証部21は、シャッフル復号証明文と暗号文と公開鍵と復号文の入力を受けて、順番の入れ替え及び暗号化である暗号文の変換内容の知識を持っていることを検証する。また、同一変換検証部21は、入力される暗号文が複数の整数の要素となる場合は、それぞれの要素が同じ順番の入れ替えと暗号化の処理とを受けたことを検証する。そして、同一変換検証部

21は、検証結果を「正当」又は「不当」として出力し、またチャレンジ（挑戦値）を生成し出力する。

【0050】置換検証部22は、シャッフル復号証明文と同一変換検証部21により生成されたチャレンジの入力を受けて、入力される暗号文に対しての順番の入れ替えが正しくなされたことを検証し、その検証結果を「正当」又は「不当」として出力する。

【0051】復号検証部23は、シャッフル復号証明文と同一変換検証部21により生成されたチャレンジの入力を受けて、シャッフル済み暗号文が秘密鍵を用いて正しく復号されて復号文が生成されたことを検証し、その検証結果を「正当」又は「不当」として出力する。

【0052】シャッフル復号検証装置20は、この同一変換検証部21、置換検証部22、復号検証部23のそれぞれの検証結果の全てが「正当」である場合には、シャッフル復号文が入力された暗号文を正しくシャッフル復号した結果であると判定し、その判定結果を「正当」と出力する。また、この検証結果の内の一つでも「不当」である場合には、その判定結果を「不当」と出力する。

【0053】以下、本実施の形態においては、ElGamal暗号を用いる実施例を用いて本発明を説明する。以下では、本発明にて前提となる事項から順に説明していく。

【0054】[ElGamal暗号方式] ElGamal暗号方式は、公開鍵暗号系に属する暗号方式である。

最初に関係

$$p = kq + 1$$

を満たしている二つの素数 p 、 q を定める。これらの素数はElGamalドメインパラメタと呼ばれる。秘密鍵

$$x \in_{\mathbb{R}} \mathbb{Z}_q$$

を \mathbb{Z}_q の要素から選ぶ。次に公開鍵

$$(g_0, m_0)$$

を位数 q の \mathbb{Z}_p^* の要素で、

$$m_0 = g_0^x \bmod p$$

この式を満たすものとして選ぶ。

【0055】 \mathbb{Z}_p^* の要素である平文

$$P \in \mathbb{Z}_p^*$$

を暗号化するには、秘密に乱数

$$s \in_{\mathbb{R}} \mathbb{Z}_q$$

を生成して暗号文を

$$(G, M) = (g_0^s, m_0^s P) \bmod p$$

と計算する。この暗号文を復号するには秘密鍵

$$x \in_{\mathbb{R}} \mathbb{Z}_q$$

を用いて、

$$P' = M / G^x \bmod p$$

と計算する。復号文 P' は、平文 P に一致する。

【0056】ここで、秘密鍵

$$x \in_{\mathbb{R}} \mathbb{Z}_q$$

が分散所持されている場合を考える。すなわち、 x が n

個の x_j ($j = 1, \dots, n$)により別個に分散所持され、

$$x = (x_1 + \dots + x_n) \bmod q$$

が成り立つ場合である。本明細書では、この x_j ($j = 1, \dots, n$)を復号用の秘密鍵と呼ぶこととする。

【0057】この時暗号文を完全に復号するには、数1の式により、 M を各復号用の秘密鍵を用いて計算した値で順に割っていく復号操作を、全ての x_j ($j = 1, \dots, n$)に関して行う。ただし、本実施例では1つの復号用の秘密鍵しか扱わないため、これを x' と表す。

【数1】

$$G^{x_j} \bmod p$$

【0058】[暗号文] 入力される n 個の暗号文を、数2により示されるものとする。それぞれの暗号文の各要素は位数 q の \mathbb{Z}_p^* の元である。

【数2】

$$(g_i, m_i) \quad i = 1, \dots, n$$

【0059】[復号文] 出力される n 個の復号文を、数2により示されるものとする。それぞれの復号文の各要素は位数 q の \mathbb{Z}_p^* の元である。

【数3】

$$(\tilde{g}_i, \tilde{m}_i) \quad i = 1, \dots, n$$

【0060】これらは、数4に示される n 個の暗号文の順番を入れ替えた後に、復号用の秘密鍵で復号したものである。

【数4】

$$(g_i, m_i) \quad i = 1, \dots, n$$

【0061】[挑戦値生成関数] 挑戦値生成関数について説明する。図5のフローチャートに示される、次のような4ステップからなる対話的証明プロトコルを考える。

【0062】まず、証明者が検証者に証明したいことに関するコミットメントを送る（ステップA1）。そして、検証者が挑戦値を証明者に送る（ステップA2）。そして、証明者は挑戦値に対して、応答を送る（ステップA3）。そして、検証者はこれらコミットメント、挑戦値、応答内容から証明の真偽を確認する（ステップA4）。

【0063】このような対話的証明プロトコルでは、証明者がどのような挑戦値に対しても適切な応答を送り返すことができることが、証明となる。ステップA2において、検証者の代わりに挑戦値を生成する関数を用いることで、上記対話的証明プロトコルを非対話的のプロトコルに変換することができる。

【0064】すなわち、図2のフローチャートに示されるように、まず証明者が、検証者に証明したいことに関

するコミットメントを生成する(ステップB1)。そして、コミットメントと証明したい内容を関数に入力して、関数の出力を挑戦値とする(ステップB2)。そして、証明者は、挑戦値に対して応答を生成し、以上の生成された各データを検証者に送る(ステップB3)。そして、検証者は、証明者から送られたこれらコミットメント、挑戦値、応答内容から証明の真偽を確認する(ステップB4)。

【0065】以上のように本発明の証明プロトコルでは、ステップB1からステップB3までの間、証明者は検証者と対話することなく証明を生成している。

【0066】上記挑戦値を生成する関数を挑戦値生成関数と呼び、これを数5により示す。

【0067】

【数5】

$$H_i(*) \quad i=1, \dots, n$$

挑戦値生成関数の出力は、 $n+1$ 個の“1”、“0”でない q 以下の整数である。また、この関数は入出力間や出力の異なる成分間の関係を、計算量的に意図して引数を決定できない関数とする。

【0068】挑戦値生成関数の具体的な構成方法の例としては、数6の式があげられる。

【数6】

$$H_i(x) = \text{Hash}((\text{Hash}(x))^i \bmod q) \bmod q$$

【0069】[置換行列] 置換行列について説明する。ここで「置換行列」を、各行各列に“0”でない成分が唯一存在し、その“0”である値を Z_q 上の“1”とする n 行 \times n 列の正方行列と定義する。例として、数7の行列があげられる。

【数7】

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【0070】[シャッフル行列] シャッフル行列を定義する。「シャッフル行列」を、 $n+1$ 行 \times $n+1$ 列の行列

$\{A_{\mu, \nu}\}$ ($\mu, \nu=0, \dots, n$)
であって、その成分が、 $\{A_{i,j}\}$ ($i, j=1, \dots, n$): n 行 \times n 列の置換行列
 $A_{0,j}, A_{i,0}, A_{0,0} \in_r Z_q$ ($i, j=1, \dots, n$)

を成すものと定義する。

【0071】[証明付シャッフル復号] 本発明の一実施例を成す証明付シャッフル復号方法について、図8を参照して説明する。

【0072】[シャッフルステップ402] 暗号文と公開鍵401

$(g_i, m_i), (g_0, m_0) : (i=1, \dots, n)$

が入力される。

【0073】次に、シャッフルステップ402にて任意のシャッフル情報403

$A_{0,j} \in_r Z_q$ ($j=1, \dots, n$)

$A_{i,j}$: 置換行列 ($i, j=1, \dots, n$)

を準備する。

【0074】次に、シャッフル済み暗号文404である数8の各変数の値を、数9の式により計算する。そして、シャッフルステップ402は、シャッフル情報403とシャッフル済み暗号文404とを出力する。

【数8】

$$(\bar{g}_i, \bar{m}_i) \quad i=1, \dots, n$$

【数9】

$$\bar{g}_i = \prod_{v=0}^n g_v^{A_{vi}} \bmod p \quad i=1, \dots, n$$

$$\bar{m}_i = \prod_{v=0}^n m_v^{A_{vi}} \bmod p \quad i=1, \dots, n$$

【0075】[復号ステップ405] シャッフル済み暗号文404と復号用の秘密鍵400とが入力される。次に、復号文406を数10の式により計算して出力する。

【数10】

$$\tilde{g}_i = \bar{g}_i \bmod p \quad i=1, \dots, n$$

$$\tilde{m}_i = \bar{g}_i^{-x} \bar{m}_i \bmod p \quad i=1, \dots, n$$

【0076】[同一変換証明ステップ407] シャッフル情報403と暗号文401と公開鍵401が入力される。次に、任意の乱数408

$A_{\mu,0} \in_r Z_q$ ($\mu=0, \dots, n$)

を準備して、コミットメントの一部である数11の各変数の値を、数12の式により計算して、同一変換証明文409として出力する。

【数11】

$$(\tilde{g}_0, \tilde{m}_0)$$

【数12】

$$\tilde{g}_0 = \prod_{v=0}^n g_v^{A_{v0}} \bmod p$$

$$\tilde{m}_0 = \prod_{v=0}^n m_v^{A_{v0}} \bmod p$$

【0077】[置換証明ステップ410] シャッフルステップ402で生成されたシャッフル情報403と同一変換証明ステップ407で生成された乱数408とから

21

22

なるシャッフル行列

 $A_{\mu, \nu} \bmod q \quad (\mu, \nu = 0, \dots, n)$

が入力される。

【0078】次に、(0, 1ではない) 任意の乱数

* $\sigma, \rho, \rho', \lambda_\mu \in_{\mathbb{R}} \mathbb{Z}_q \quad (\mu = 0, \dots, n)$ $g = g_0$

を準備して、数13を計算する。

* 【数13】

$$\phi_i = \sum_{j=1}^n (3A_{j0} + \rho'\lambda_j) A_{ji} \bmod q \quad i = 1, \dots, n$$

$$\phi_i = \sum_{j=1}^n (3A_{j0} + 2\rho'\lambda_j) A_{j0} A_{ji} + \rho A_{0i} \bmod q \quad i = 1, \dots, n$$

$$\phi_0 = \sum_{j=1}^n (A_{j0} + \rho'\lambda_j) A_{j0} A_{j0} + \rho'\lambda_0 + \rho A_{00} \bmod q$$

$$\psi_i = \sum_{j=1}^n 2A_{j0} A_{ji} + \sigma A_{0i} \bmod q \quad i = 1, \dots, n$$

$$\psi_0 = \sum_{j=1}^n A_{j0} A_{j0} + \sigma A_{00} \bmod q$$

$$v = g^{\rho}, v' = g^{\rho'}, \dot{v}_0 = g^{\phi_0}, \dot{v}_i = g^{\phi_i},$$

$$w = g^{\sigma}, \dot{w}_0 = g^{\psi_0}, \dot{w}_i = g^{\psi_i},$$

$$\dot{u}_i = g^{\phi_i}, u_0 = g^{\lambda_0}, u_i = g^{\lambda_i} \bmod p \quad i = 1, \dots, n$$

【0079】ここで数14の各変数の値を、置換証明文 ※ 【数14】

411として出力する。

$$v, \dot{v}_0, \dot{v}_i, w, \dot{w}_0, \dot{w}_i, v', \dot{u}_i, u_0, u_i \quad i = 1, \dots, n$$

【0080】[リスpons生成ステップ412] 暗号文 ★の式により計算する。

と公開鍵401と同一変換証明文409と置換証明文4 【数15】

11と復号文406とが入力され、チャレンジを数15★

$$c_i = H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j,$$

$$v, \dot{v}_0, \dot{v}_j, w, \dot{w}_0, \dot{w}_j, v', \dot{u}_j, u_0, u_j$$

$$j = 1, \dots, n) \quad , \quad i = 1, \dots, n$$

【0081】次にリスponsを、数16の式により計算する。

【数16】

$$r_\mu = \sum_{\nu=0}^n A_{\mu\nu} c_\nu \bmod q \quad \mu = 0, \dots, n$$

$$\lambda = \lambda_0 + \sum_{i=1}^n \lambda_i r_i \bmod q$$

【0082】最後に、同一変換証明文と置換証明文とリスponsとをシャッフル証明文413として出力する。

【0083】[復号証明ステップ417] 復号文406 50 【0084】次に、復号証明のチャレンジを、数18の

と復号用の秘密鍵400とリスpons生成ステップで生成されたチャレンジ414とが入力される。任意の

 $\beta \in_{\mathbb{R}} \bmod q$

を選び、次に、数17の式を計算する。

【数17】

$$\zeta = \prod_{i=1}^n \tilde{g}_i^{c_i} \bmod p$$

$$\eta = \zeta^{x'} \bmod p$$

$$\eta' = \zeta^{\beta} \bmod p$$

$$m_0^* = g_0^{\beta} \bmod p$$

式により計算する。

【数18】

$$c' = H_0(\zeta, \eta, \eta', g_0, m'_0, m''_0)$$

【0085】次に、復号証明のレスポンスを

$$r' = c' \cdot x' + \beta \pmod{q}$$

と計算する。最後に復号の証明文415として、

η, η', m_0'', r'

を出力する。

【0086】【証明文】同一変換証明文と置換証明文と*10 【数19】

$$c_i = H_i(g_0, g_j, m_0, m_j, \tilde{g}_0, \tilde{g}_j, \tilde{m}_0, \tilde{m}_j, v,$$

$$\dot{v}_0, \dot{v}_j, w, \dot{w}_0, \dot{w}_j, v', \dot{u}_j, u_0, u_j$$

$$j=1, \dots, n) \quad i=1, \dots, n$$

【0089】次に、数20の式が成り立てば「正当」を、成り立たなければ「不当」を出力501する。

【数20】

$$\prod_{\mu=0}^n g_{\mu}^{r_{\mu}} = \prod_{v=0}^n \tilde{g}_v^{c_v} \pmod{p}$$

$$\prod_{\mu=0}^n m_{\mu}^{r_{\mu}} = \eta \prod_{v=0}^n \tilde{m}_v^{c_v} \pmod{p}$$

$$u^{\lambda} = \dot{u}_0 \prod_{i=1}^n \dot{u}_i^{r_i r_i} \pmod{p}$$

$$v'^{\lambda} v^{r_0} g^{\sum_{i=1}^n (r_i^3 - c_i^3)} = \dot{v}_0 \prod_{i=1}^n \dot{u}_i^{c_i^2} \prod_{i=1}^n \dot{v}_i^{c_i} \pmod{p}$$

$$w^{r_0} g^{\sum_{i=1}^n (r_i^2 - c_i^2)} = \dot{w}_0 \prod_{i=0}^n \dot{w}_i^{c_i} \pmod{p}$$

【0091】【復号検証ステップ】シャッフル復号証明文と同一変換検証ステップで求められたチャレンジ500が入力される。次に、補助のチャレンジを次の数22の式により計算する。

【数22】

$$c' = H_0(\zeta, \eta, \eta', g_0, m'_0, m''_0)$$

【0092】次に、数23の式が成り立てば「正当」を、成り立たなければ「不当」を出力503する。

【数23】

* レスポンスと復号証明文を、シャッフル復号の証明文416として出力する。

【0087】【シャッフル復号検証】本実施の形態のシャッフル復号検証方法について、図3を参照して説明する。

【0088】【同一変換検証ステップ】シャッフル復号証明文416と暗号文と公開鍵401と復号文が入力される。チャレンジ500を、数19の式により計算する。

【数19】

※【0090】【置換検証ステップ】シャッフル復号証明文と同一変換検証ステップで求められたチャレンジ500が入力される。次に、数21の式が成り立てば「正当」を、成り立たなければ「不当」を出力502する。

20 【数21】

$$g_0^{r'} = m'_0 c' m''_0 \pmod{p}$$

$$\left(\prod_{i=1}^n \tilde{g}_i^{c_i} \right)^{r'} = \eta^{c'} \eta' \pmod{p}$$

40

【0093】同一変換検証ステップと置換検証ステップと復号検証ステップとの、全ての出力が正当であれば「正当」を、一つでも「不当」があれば「不当」を、シャッフル復号検証の出力504とする。

【0094】なお、本実施の形態の証明付シャッフル復号システムは、証明付シャッフル復号装置10のシャッフル部11、復号部12、証明部13、同一変換証明部13-1、置換証明部13-2、レスポンス生成部13-3、復号証明部13-4の機能や、シャッフル復号検

50

証装置 20 の同一変換検証部 21、置換検証部 22、復号検証部 23 の機能や、その他の機能をハードウェア的に実現することは勿論として、各機能を備えるコンピュータプログラムである証明付シャッフル復号プログラム及びシャッフル復号検証プログラムを、コンピュータ処理装置のメモリにロードされることで実現することができる。この証明付シャッフル復号プログラム及びシャッフル復号検証プログラムは、磁気ディスク、半導体メモリその他の記録媒体 80、90 に格納される。そして、その記録媒体からコンピュータ処理装置にロードされ、コンピュータ処理装置の動作を制御することにより、上述した各機能を実現する。

【0095】以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【0096】

【発明の効果】以上説明したように本発明によれば、証明付シャッフルに証明付復号を追加した場合の計算量を、従来の技術と比べて大きく削減することができる。

【0097】例えば、入力暗号文の数を n とした時、文献 2 の従来技術を用いて証明付シャッフルに証明付復号を追加した場合には、乗剰余演算が $3n$ 回必要とされていたのに対して、本発明によれば乗剰余演算は $n+3$ 回で済み、従来の技術よりも大幅に乗剰余演算の回数を削減することができる。

【0098】更に、本発明において行う乗剰余演算は、従来の技術における個別の乗剰余演算ではなく、乗剰余演算の積の計算であることから、個別の乗剰余演算よりも遙かに少ない計算量で計算することができ、更なる高速化を実現することができる。

*

* 【図面の簡単な説明】

【図 1】 本発明の一実施の形態による証明付シャッフル復号システムの構成を示すブロック図である。

【図 2】 本発明の一実施の形態による証明付シャッフル復号システムの処理を説明するためのフローチャートである。

【図 3】 本発明の一実施の形態による証明付シャッフル復号を説明するための図である。

10 【図 4】 本発明の一実施の形態によるシャッフル復号検証を説明するための図である。

【図 5】 従来の技術における処理を説明するためのフローチャートである。

【図 6】 従来の証明付シャッフルの処理を説明するための図である。

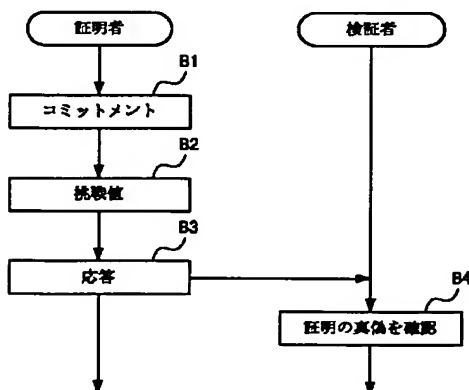
【図 7】 従来の証明付復号の処理を説明するための図である。

【図 8】 図 6 と図 7 の従来の技術を組み合わせた構成を示す図である。

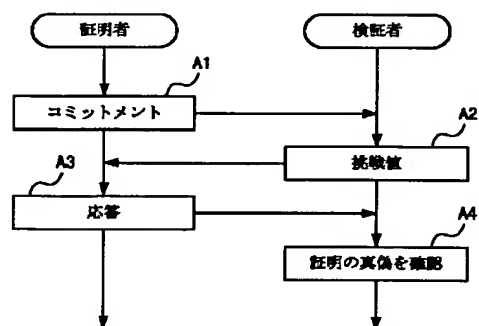
【符号の説明】

- 20 10 証明付シャッフル復号装置
11 シャッフル部
12 復号部
13 証明部
13-1 同一変換証明部
13-2 置換証明部
13-3 リスpons生成部
13-4 復号証明部
20 シャッフル復号検証装置
21 同一変換検証部
22 置換検証部
23 復号検証部
80、90 記録媒体

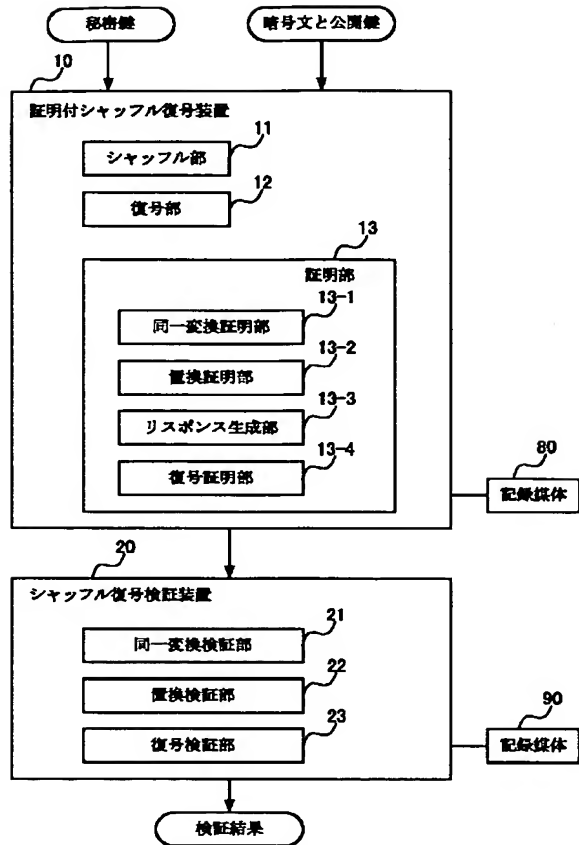
【図 2】



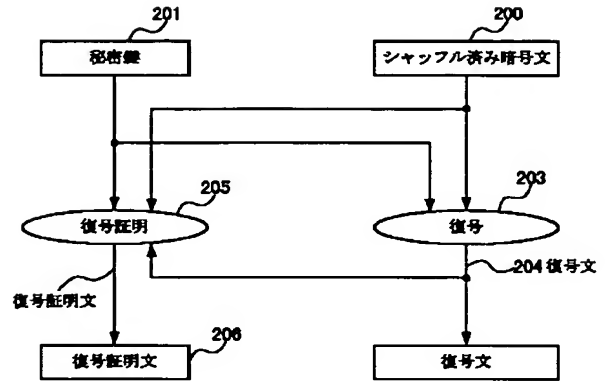
【図 5】



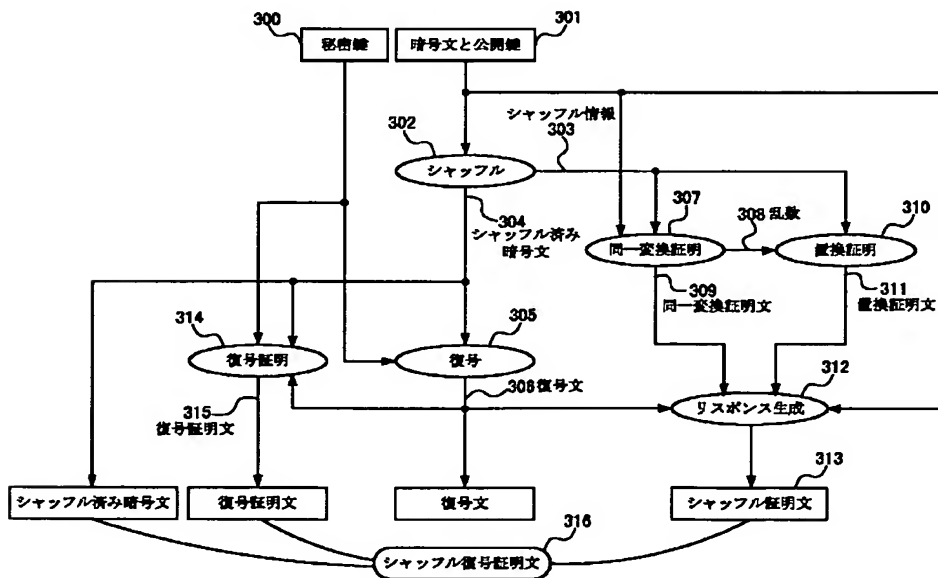
【図1】



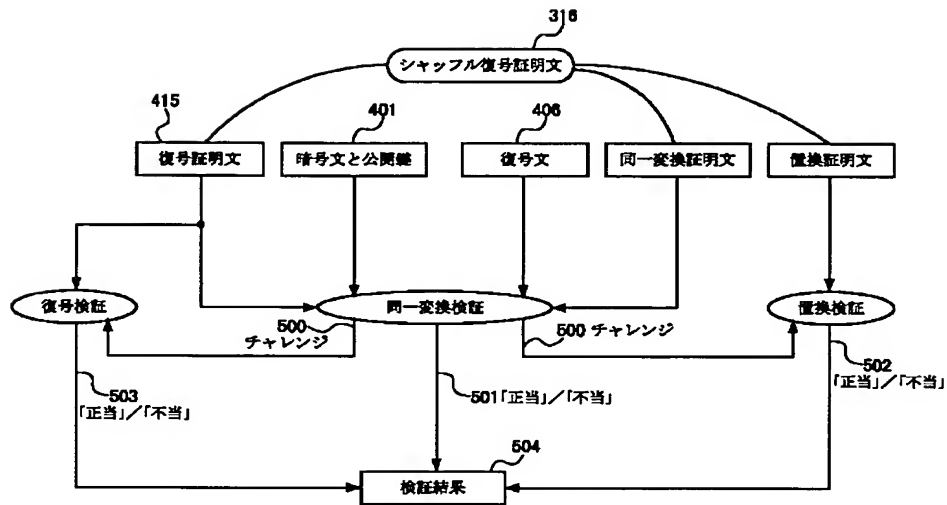
【図7】



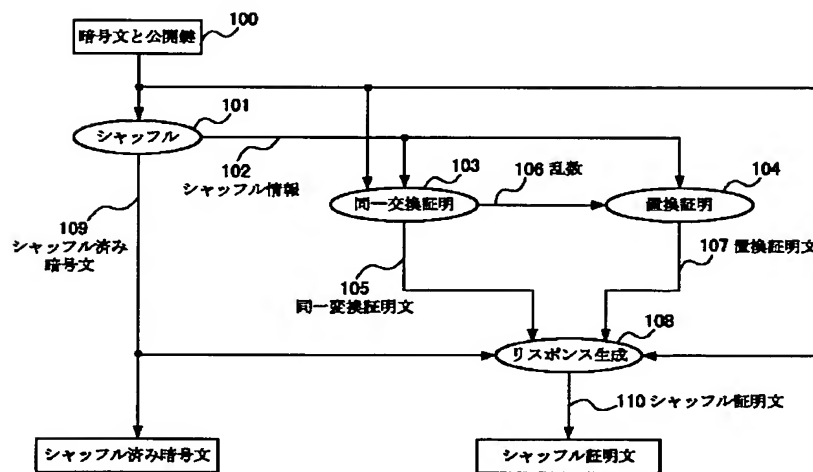
【図3】



【図4】



【図6】



【図8】

